UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI

DANIEL BROWN, IMAN AYUK, KERRY LOVELL, and RICHARD MEADE individually and on behalf of all others similarly situated, Plaintiffs, v. Ascension Health, Defendant.	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Daniel Brown, Iman Ayuk, Kerry Lovell. And Richard Meade ("Plaintiffs") individually and on behalf of all others similarly situated, by and through their undersigned counsel, bring this Class Action Complaint against Ascension Health ("Ascension"). Plaintiffs allege the following upon information and belief based on and the investigation of counsel, except as to those allegations that specifically pertain to Plaintiffs, which are alleged upon personal knowledge.

INTRODUCTION

1. Plaintiffs and the proposed Class Members bring this class action lawsuit on behalf of all persons who entrusted Ascension with sensitive personally identifiable information ("PII")[1] and protected health information ("PHI", and collectively with PII, "Private Information") that was impacted in a data breach (the "Data Breach" or the "Breach").

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

2. Plaintiffs' claims arise from Defendant's failure to properly secure and safeguard Private Information that was entrusted to it, and its accompanying responsibility to store and transfer that information.

3. Ascension is a Catholic health-system that includes approximately 134,000 associates, 35,000 affiliated providers and 140 hospitals, serving communities in 19 states and the District of Columbia.[2]

4. Defendant had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on their affirmative representations to Plaintiffs and the Class, to keep their Private Information confidential, safe, secure, and protected from unauthorized disclosure or access.

5. Defendant failed to take precautions designed to keep its patients' Private Information secure.

6. Defendant owed Plaintiffs and Class Members a duty to take all reasonable and necessary measures to keep the Private Information it collected safe and secure from unauthorized access. Defendant solicited, collected, used, and derived a benefit from the Private Information, yet breached its duty by failing to implement or maintain adequate security practices.

7. Defendant admits that information in its system was accessed by unauthorized individuals, though it provided little information regarding how the Data Breach occurred.

8. The sensitive nature of the data exposed through the Data Breach signifies that Plaintiffs and Class Members have suffered irreparable harm. Plaintiffs and Class Members have lost the ability to control their private information and are subject to an increased risk of identity theft.

[2] *About Ascension*, ASCENSION, https://about.ascension.org/about-us (last visited May 22, 2024).

9. Defendant, despite having the financial wherewithal and personnel necessary to prevent the Data Breach, nevertheless failed to use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it maintained for Plaintiffs and Class Members, causing the exposure of Private Information for Plaintiffs and Class Members.

10. As a result of the Defendant's inadequate digital security and notice process, Plaintiffs and Class Members' Private Information was exposed to criminals. Plaintiffs and the Class have suffered and will continue to suffer injuries including: financial losses caused by misuse of Private Information; the loss or diminished value of their Private Information as a result of the Data Breach; lost time associated with detecting and preventing identity theft; and theft of personal and financial information.

11. Moreover, as an ongoing harm resulting from the Data Breach, Plaintiffs and Class Members experienced disruptions in services because Ascension's network systems were offline and inaccessible to patients. These disruptions included delays in obtaining prescription medications, inability to access patient health records via Ascension's MyChart patient portal, cancellation of medical appointments with providers, and inability to schedule medical appointments.

12. Plaintiffs bring this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; (iii) effectively secure hardware containing protected Private Information using reasonable and adequate security procedures free of vulnerabilities and incidents; and (iv) timely notify Plaintiffs and Class Members of the Data Breach. Defendant's conduct amounts to at least negligence and violates federal and state statutes.

13. Plaintiffs bring this action individually and on behalf of a Nationwide Class of

similarly situated individuals against Defendant for: negligence; negligence per se; unjust enrichment, breach of implied contract, and breach of implied covenant of good faith and fair dealing, invasion of confidence, and violation of the Missouri Merchandise Practices Act, Mo. Rev. Stat. §§ 407.010, *et seq.*

14. Plaintiffs seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

PARTIES

Plaintiffs

15. Plaintiff Daniel Brown is a citizen of Kansas and resides in Coffeyville. Plaintiff is a patient of Ascension St. John Phillips in Bartlesville, Oklahoma, and was impacted by the Data Breach. On May 17, 2024, Plaintiff was scheduled to have a sleep study done. As a result of the Data Breach, plaintiff Brown was unable to proceed with his scheduled sleep study, and unable to reschedule the sleep study appointment. Furthermore, plaintiff Brown was unable to access his patient health records via Ascension's patient portal. As a consequence of the Data Breach, plaintiff Brown has been forced to, and will continue to, invest significant time monitoring his accounts to detect and reduce the consequences of likely identity fraud. As a result of the Data Breach, plaintiff Brown is now subject to substantial and imminent risk of future harm. Plaintiff Brown would not have used Defendant's services had he known that it would expose his sensitive Private Information.

16. Plaintiff Iman Ayuk is a citizen of Michigan and resides in Taylor. Plaintiff is a patient of Ascension Providence Hospital in Southfield, Michigan and was impacted by the Data Breach. As a consequence of the Data Breach, plaintiff Ayuk was unable to access her Ascension

patient portal to contact her medical providers and view her patient health records. Furthermore, as a consequence of the Data Breach, plaintiff Ayuk has been forced to, and will continue to, invest significant time monitoring her accounts to detect and reduce the consequences of likely identity fraud. As a result of the Data Breach, plaintiff Ayuk is now subject to substantial and imminent risk of future harm. Plaintiff Ayuk would not have used Defendant's services had she known that it would expose her sensitive Private Information.

17. Plaintiff Kerry Lovell is a citizen of Wisconsin and resides in Racine. Plaintiff is a patient of Ascension All Saints Hospital in Racine, Wisconsin and was impacted by the Data Breach. As a result of the Data Breach, plaintiff Lovell was unable to access her patient health records via Ascension's patient portal or communicate with her providers. Furthermore, plaintiff Lovell was unable to obtain prescriptions refills online. As a consequence of the Data Breach, plaintiff Lovell has been forced to, and will continue to, invest significant time monitoring her accounts to detect and reduce the consequences of likely identity fraud. As a result of the Data Breach, plaintiff Lovell is now subject to substantial and imminent risk of future harm. Plaintiff Lovell would not have used Defendant's services had she known that it would expose her sensitive Private Information.

18. Plaintiff Richard Meade is a citizen of Illinois and resides in Lockport. Plaintiff is a patient of Ascension St. Joseph Phillips in Joliet, Illinois and was impacted by the Data Breach. As a result of the Data Breach, plaintiff Meade was unable to access his patient health records via Ascension's patient portal. As a consequence of the Data Breach, plaintiff Meade has been forced to, and will continue to, invest significant time monitoring his accounts to detect and reduce the consequences of likely identity fraud. As a result of the Data Breach, plaintiff Meade is now subject to substantial and imminent risk of future harm. Plaintiff Meade would not have used Defendant's services had he known that it would expose his sensitive Private Information.

Defendant

19. Defendant Ascension Health is a Missouri non-profit corporation with its principal place of business located in St. Louis, Missouri. Defendant is the largest non-profit, Catholic health-system in the United States that "includes approximately 134,000 associates, 35,000 affiliated providers and 140 hospitals, serving communities in 19 states and the District of Columbia."[3]

JURISDICTION AND VENUE

20. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. At least one member of the Class defined below is a citizen of a different state than Defendant, and there are more than 100 putative Class Members.

21. This Court has personal jurisdiction over Defendant because Defendant is registered to do business, and maintains its principal place of business, in St. Louis, Missouri.

22. Venue is proper in these District under 28 U.S.C. § 1391(b)(2) because Defendant is headquartered in this District, and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

A. Background on Defendant

23. Defendant is a Catholic health-system that "includes approximately 134,000 associates, 35,000 affiliated providers and 140 hospitals, serving communities in 19 states and the District of Columbia."[4]

24. In the ordinary course of its business practices, Defendant stores, maintains, and

[3] *About Ascension*, ASCENSION, https://about.ascension.org/about-us (last visited May 22, 2024).
[4] *Id.*

uses an individuals' Private Information.

25. Upon information and belief, Defendant made promises and representations to its patients, including Plaintiffs and Class Members, that the Private Information collected from them would be kept safe, confidential, and that the privacy of that information would be maintained.

26. Plaintiffs and Class Members provided their Private Information to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

27. As a result of collecting and storing the Private Information of Plaintiffs and Class Members for its own financial benefit, Defendant had a continuous duty to adopt and employ reasonable measures to protect Plaintiffs' and the Class Members' Private Information from disclosure to third parties.

B. The Data Breach

28. On or around May 8, 2024, Defendant detected unusual activity on several of its IT systems.[5] In response, Ascension secured its systems and then launched an investigation with the help of third-party data security experts.[6] On May 9, 2024, Defendant posted a notice on its website providing information on the Data Breach, its response, and subsequent investigation into the Data Breach.[7]

29. The investigation determined that the Data Breach affected operation at all 142 of Ascension's hospitals and systems impacted including electronic medical records accessibility, phone systems, and systems used to book tests, procedures, and medications, and

[5] The "Online Notice." *Cybersecurity Event Update*, ASCENSION (May 21, 2024) https://about.ascension.org/news/2024/05/network-interruption-update (last visited May 22, 2024).
[6] *Id.*
[7] *Id.*

elective procedures.[8]

30. Plaintiffs' claims arise from Defendant's failure to safeguard Private Information provided by and belonging to its patients and failure to provide timely notice of the Data Breach.

31. Defendant failed to take precautions designed to keep their patients' Private Information secure.

32. While Defendant sought to minimize the damage caused by the Data Breach, it cannot and has not denied that there was unauthorized access to the sensitive Private Information of Plaintiffs and Class Members.

33. Individuals affected by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

C. Defendant's Failure to Prevent, Identify and Timely Report the Data Breach

34. Defendant admits that unauthorized third persons accessed its network systems.

35. Defendant failed to take adequate measures to protect its computer systems against unauthorized access.

36. Defendant was not only aware of the importance of protecting the Private Information that it maintains, as alleged, it promoted its capability to do so, as evident from its Privacy Policy.[9]

37. Defendant provides on its website that:

> Our Commitment: "We are committed to maintaining the privacy and confidentiality of your health information."
>
> Our responsibilities: "We are required by law to maintain the privacy and security of your health information."[10]

[8] Steve Adler, *Ascension Ransomware Attack Affecting All 142 Hospitals*, The HIPAA Journal (May 13, 2024) https://www.hipaajournal.com/ascension-cyberattack-2024/ (last visited May 22, 2024).
[9] See *Website Privacy Policy,* ASCENSION, https://about.ascension.org/privacy (Last visited May 22, 2024).
[10] *Id.*

38. The Private Information that Defendant allowed to be exposed in the Data Breach is the type of private information that Defendant knew or should have known would be the target of cyberattacks.

39. Despite its own knowledge of the inherent risks of cyberattacks, and notwithstanding the FTC's data security principles and practices,[11] Defendant failed to disclose that its systems and security practices were inadequate to reasonably safeguard its past and present patients' sensitive Personal Information.

40. The FTC directs businesses to use an intrusion detection system to expose a breach as soon as it occurs, monitor activity for attempted hacks, and have an immediate response plan if a breach occurs.[12] Immediate notification of a Data Breach is critical so that those impacted can take measures to protects themselves.

D. Data Breaches Cause Disruptions That Put Patients at an Increased Risk of Harm

41. Cyber-attacks at medical facilities such as Defendant's are especially problematic because of the disruption they cause to the health treatment and overall daily lives of patients affected by the attack.

42. For instance, loss of access to patient histories, charts, images, and other information forces providers to limit or cancel patient treatment due to a disruption of service. This leads to a deterioration in the quality of overall care patients receive at facilities affected by cyber-attacks and related data breaches.

[11] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited May 22, 2024).
[12] *Id.*

43. Researchers have found medical facilities that experience a data security incident incur an increase in the death rate among patients' months and years after the attack.[13] Researchers have further found that at medical facilities that experience a data breach, the incident leads to a deterioration in patient outcomes, generally.[14]

44. Similarly, cyber-attacks and related data security incidents inconvenience patients; these inconveniences include, but are not limited, to the following:

a. rescheduling of medical treatment;

b. being forced to find alternative medical care and treatment;

c. delays or outright cancellation of medical care and treatment;

d. undergoing medical care and treatment without medical providers having access to a complete medical history and records; and

e. the indefinite loss of personal medical history.

E. The Harm Caused by the Data Breach Now and Going Forward

45. Victims of data breaches are susceptible to becoming victims of identity theft. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority," 17 C.F.R. § 248.201(9), and when "identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[15]

46. The type of data that may have been accessed and compromised here – such as, full names and Social Security numbers – can be used to perpetrate fraud and identity theft. Social

[13] See Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019) https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks (last accessed May 23, 2024).

[14] See Sung J. Choi PhD., et al., *Data breach remediation efforts and their implications for hospital quality*, HEALTH SERVICES RESEARCH (Sept. 10, 2019) https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203 (last accessed May 23, 2024).

[15] *Prevention and Preparedness*, NEW YORK STATE POLICE, https://troopers.ny.gov/prevention-and-preparedness (last visited May 22, 2024).

Security numbers are widely regarded as the most sensitive information hackers can access. Social Security numbers and dates of birth together constitute high risk data.

47. Plaintiffs and Class members face a substantial risk of identity theft given that their Social Security numbers, addresses, dates of birth, and other important Private Information were compromised in the Data Breach. Once a Social Security number is stolen, it can be used to identify victims and target them in fraudulent schemes and identity theft.

48. Stolen Private Information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal their identities and online activity.

49. When malicious actors infiltrate companies and copy and exfiltrate the Private Information that those companies store, the stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[16]

50. For example, when the U.S. Department of Justice announced their seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [PII] belonging to victims from countries all over the world. One of the key challenges of protecting PII online is their pervasiveness. As data breaches in the news continue to reveal, PII about employees, customers and the public are housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[17]

---

[16] *Shining a Light on the Dark Web with Identity Monitoring*, IDENTITYFORCE (Dec. 28, 2020) https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited May 22, 2024).

[17] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, ARMOR (April 3, 2018) https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last visited May 22, 2024).

51. PII remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[18] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[19]

52. A compromised or stolen Social Security number cannot be addressed as simply as a stolen credit card. An individual cannot obtain a new Social Security number without significant work. Preventive action to defend against the possibility of misuse of a Social Security number is not permitted; rather, an individual must show evidence of actual, ongoing fraud activity to obtain a new number. Even then, however, obtaining a new Social Security number may not suffice. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[20]

53. The Private Information compromised in the Data Breach demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained: "[c]ompared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[21]

54. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in

---

[18] *Id.*

[19] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015) https://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited May 22, 2024).

[20] *Id.*

[21] *Experts advise compliance not same as security*, RELIAS MEDIA (Mar. 1, 2015) https://www.reliasmedia.com/articles/134827-experts-advise-compliance-not-same-as-security (last visited May 22, 2024).

2019, resulting in more than $3.5 billion in losses to individuals and business victims.[22]

55. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[23] Defendant did not rapidly report to Plaintiffs and Class Members that their Private Information had been stolen.

56. As a result of the Data Breach, the Private Information of Plaintiffs and Class Members have been exposed to criminals for misuse. The injuries suffered by Plaintiffs and Class Members, or likely to be suffered thereby as a direct result of Defendant's Data Breach, include: (a) theft of their Private Information; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of this Breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft resulting from their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damage to and diminution in value of their personal data entrusted to Defendant with the mutual understanding that Defendant would safeguard their Private Information against theft and not allow access to and misuse of their personal data by any unauthorized third party; and (h) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further injurious breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

---

[22] *2019 Internet Crime Report Released*, FBI (Feb. 11, 2020) https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120#:~:text=IC3%20received%20467%2C361%20complaints%20in,%2Ddelivery%20scams%2C%20and%20extortion (last visited May 22, 2024).

[23] *Id.*

57. In addition to a remedy for economic harm, Plaintiffs and Class Members maintain an interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

58. Defendant disregarded the rights of Plaintiffs and Class Members by (a) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (b) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiffs' and Class Members' Private Information; (c) failing to take standard and reasonably available steps to prevent the Data Breach; (d) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (e) failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

59. The actual and adverse effects to Plaintiffs and Class Members, including the imminent, immediate, and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly and/or proximately caused by Defendant's wrongful actions and/or inaction and the resulting Data Breach require Plaintiffs and Class Members to take affirmative acts to recover their peace of mind and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts, for which there is a financial and temporal cost. Plaintiffs and other Class Members have suffered, and will continue to suffer, such damages for the foreseeable future.

CLASS ALLEGATIONS

60. Plaintiffs bring this action pursuant to Rule 23 of the Federal Rules of Civil Procedure, individually and on behalf of the following Nationwide Class:

> All persons in the United States whose personal information was compromised in the Data Breach publicly announced by Defendant in May of 2024 (the "Class").

61. Plaintiffs also seeks certification of a Missouri Subclass, defined as follows:

> All Missouri residents whose personal information was compromised in the Data Breach publicly announced by Defendant in May of 2024 (the "Missouri Subclass").

62. Specifically excluded from the Class are Defendant, its officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint venturers, or entities controlled by Defendant, and its heirs, successors, assigns, or other persons or entities related to or affiliated with Defendant and/or its officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

63. Plaintiffs reserve the right to amend the Class definitions above if further investigation and/or discovery reveals that the Class should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

64. This action may be certified as a class action under Federal Rule of Civil Procedure 23 because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

65. Numerosity (Rule 23(a)(1)): The Class is so numerous that joinder of all Class Members is impracticable. Although the precise number of such persons is unknown, and the facts are presently within the sole knowledge of Defendant, upon information and belief, Plaintiffs estimate that the Class is comprised of hundreds of thousands of Class Members, if not more. The Class is sufficiently numerous to warrant certification.

66. Typicality of Claims (Rule 23(a)(3)): Plaintiffs' claims are typical of those of other Class Members because, Plaintiffs, like the unnamed Class, had their Private Information compromised as a result of the Data Breach. Plaintiffs are members of the Class, and their claims are typical of the claims of the members of the Class. The harm suffered by Plaintiffs is similar to that suffered by all other Class Members which was caused by the same misconduct by Defendant.

67. Adequacy of Representation (Rule 23(a)(4)): Plaintiffs will fairly and adequately represent and protect the interests of the Class. Plaintiffs have no interests antagonistic to, nor in conflict with, the Class. Plaintiffs have retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

68. Superiority (Rule 23(b)(3)): A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class Members is relatively small, the expense and burden of individual litigation make it impossible for individual Class Members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendant will likely continue its wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for its wrongdoing as asserted herein.

69. Predominant Common Questions (Rule 23(a)(2)): The claims of all Class Members present common questions of law or fact, which predominate over any questions affecting only individual Class Members, including:

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

g. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

h. Whether Defendant's storage of Class Member's Private Information was done in a negligent manner;

i. Whether Defendant had a duty to protect and safeguard Plaintiffs' and Class Members' Private Information;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's conduct violated Plaintiffs' and Class Members' privacy;

l. Whether Defendant's conduct violated the statutes as set forth herein;

m. Whether Defendant took sufficient steps to secure its customers' Private Information;

n. Whether Defendant was unjustly enriched;

o. The nature of relief, including damages and equitable relief, to which Plaintiffs and Class Members are entitled.

70. Information concerning Defendant's policies is available from Defendant's records.

71. Plaintiffs know of no difficulty which will be encountered in the management of this litigation which would preclude its maintenance as a class action.

72. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendant. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

73. Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

74. Given that Defendant had not indicated any changes to its conduct or security measures, monetary damages are insufficient and there is no complete and adequate remedy at law.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and All Class Members)

75. Plaintiffs incorporate by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 14 and paragraphs 23 through 59 as though fully set forth herein.

76. Plaintiffs bring this claim individually and on behalf of the Class Members.

77. Defendant knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

78. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' and Class Members' Private Information.

79. Defendant had, and continues to have, a duty to timely disclose that Plaintiffs' and Class Members' Private Information within its possession was compromised and precisely the types of information that were compromised.

80. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected its patients' Private Information.

81. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its patients. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiffs and Class Members from a data breach.

82. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

83. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' Private Information.

84. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' and Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems; and

c. Failing to periodically ensure that its computer systems and networks had plans in place to maintain reasonable data security safeguards.

85. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within Defendant's possession.

86. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiffs' and Class Members' Private Information.

87. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiffs and Class Members that the Private Information within Defendant's possession might have been compromised and precisely the type of information compromised.

88. Defendant breached the duties set forth in 15 U.S.C. § 45, the FTC guidelines, the NIST's Framework for Improving Critical Infrastructure Cybersecurity, and other industry guidelines. In violation of 15 U.S.C. § 45, Defendant failed to implement proper data security procedures to adequately and reasonably protect Plaintiffs' and Class Members' Private

Information. In violation of the FTC guidelines, *inter alia,* Defendant did not protect the personal patient information it keeps; failed to properly dispose of personal information that was no longer needed; failed to encrypt information stored on computer networks; lacked the requisite understanding of its networks' vulnerabilities; and failed to implement policies to correct security issues.

89. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

90. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiffs' and Class Members' Private Information would result in injury to Plaintiffs and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

91. It was foreseeable that the failure to adequately safeguard Plaintiffs' and Class Members' Private Information would result in injuries to Plaintiffs and Class Members.

92. Defendant's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised.

93. But for Defendant's negligent conduct and breach of the above-described duties owed to Plaintiffs and Class Members, their Private Information would not have been compromised.

94. As a result of Defendant's failure to timely notify Plaintiffs and Class Members that their Private Information had been compromised, Plaintiffs and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

95. As a result of Defendant's negligence and breach of duties, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes, and Plaintiffs and Class Members

have and will suffer damages including: a substantial increase in the likelihood of identity theft; the compromise, publication, and theft of their personal information; loss of time and costs associated with the prevention, detection, and recovery from unauthorized use of their personal information; the continued risk to their personal information; future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the personal information compromised as a result of the Data Breach; and overpayment for the services or products that were received without adequate data security.

COUNT II
UNJUST ENRICHMENT
(On behalf of Plaintiffs and All Class Members)

96. Plaintiffs incorporate by reference and re-allege each and every allegation set forth above in paragraphs 1 through 14 and paragraphs 23 through 59 as though fully set forth herein.

97. Plaintiffs and Class Members conferred a benefit upon Defendant by using Defendant's services.

98. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiffs. Defendant also benefited from the receipt of Plaintiffs' and Class Members' Private Information, as this was used for Defendant to administer its services to Plaintiffs and the Class.

99. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' and the Class Members' services and their Private Information because Defendant failed to adequately protect their Private Information. Plaintiffs and the proposed Class would not have provided their Private Information to Defendant or utilized its services had they known Defendant would not adequately protect their Private Information.

100. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and the Class all unlawful or inequitable proceeds received by it because of its misconduct and Data Breach.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and All Class Members)

101. Plaintiffs incorporate by reference and re-allege each and every allegation set forth above in paragraphs 1 through 14 and paragraphs 23 through 59 as though fully set forth herein.

102. Plaintiffs and the Class provided and entrusted their Private Information to Defendant. Plaintiffs and the Class provided their Private Information to Defendant as part of Defendant's regular business practices.

103. In so doing, Plaintiffs and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen, in return for the business services provided by Defendant. Implied in these exchanges was a promise by Defendant to ensure that the Private Information of Plaintiffs and Class Members in its possession was secure.

104. Pursuant to these implied contracts, Plaintiffs and Class Members provided Defendant with their Private Information in order for Defendant to provide services, for which Defendant is compensated. In exchange, Defendant agreed to, among other things, and Plaintiffs and the Class understood that Defendant would: (1) provide services to Plaintiffs and Class Members; (2) take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class Members' Private Information; and (3) protect Plaintiffs' and Class Members' Private Information in compliance with federal and state laws and regulations and industry standards.

105. Implied in these exchanges was a promise by Defendant to ensure the Private Information of Plaintiffs and Class Members in its possession was only used to provide the agreed-upon reasons, and that Defendant would take adequate measures to protect Plaintiffs' and Class Members' Private Information.

106. A material term of this contract is a covenant by Defendant that it would take reasonable efforts to safeguard that information. Defendant breached this covenant by allowing Plaintiffs' and Class Members' Private Information to be accessed in the Data Breach.

107. Indeed, implicit in the agreement between Defendant and its patients was the obligation that both parties would maintain information confidentially and securely.

108. These exchanges constituted an agreement and meeting of the minds between the parties: Plaintiffs and Class Members would provide their Private Information in exchange for services by Defendant. These agreements were made by Plaintiffs and Class Members as Defendant's patients.

109. When the parties entered into an agreement, mutual assent occurred. Plaintiffs and Class Members would not have disclosed their Private Information to Defendant but for the prospect of utilizing Defendant's services. Conversely, Defendant presumably would not have taken Plaintiffs' and Class Members' Private Information if it did not intend to provide Plaintiffs and Class Members with its services.

110. Defendant was therefore required to reasonably safeguard and protect the Private Information of Plaintiffs and Class Members from unauthorized disclosure and/or use.

111. Plaintiffs and Class Members accepted Defendant's offer of services and fully performed their obligations under the implied contract with Defendant by providing their Private Information, directly or indirectly, to Defendant, among other obligations.

112. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their Private Information.

113. Defendant breached the implied contracts with Plaintiffs and Class Members by failing to reasonably safeguard and protect Plaintiffs' and Class Members' Private Information.

114. Defendant's failure to implement adequate measures to protect the Private Information of Plaintiffs and Class Members violated the purpose of the agreement between the parties.

115. Instead of spending adequate financial resources to safeguard Plaintiffs' and Class Members' Private Information, which Plaintiffs and Class Members were required to provide to Defendant, Defendant instead used that money for other purposes, thereby breaching their implied contracts it had with Plaintiffs and Class Members.

116. As a proximate and direct result of Defendant's breaches of their implied contracts with Plaintiffs and Class Members, Plaintiffs and the Class Members suffered damages as described in detail above.

COUNT IV
BREACH OF THE IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING
(On behalf of Plaintiffs and All Class Members)

117. Plaintiffs incorporate by reference and re-allege each and every allegation set forth above in paragraphs 1 through 14 and paragraphs 23 through 59 as though fully set forth herein.

118. Defendant has violated the covenant of good faith and fair dealing by its conduct alleged herein.

119. Every contract in this state has an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

120. Plaintiffs and Class Members have complied with and performed all, or substantially all, of the obligations imposed on their conditions of services with Defendant.

121. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard its patients Private Information, failing to timely and accurately disclose the Data Breach to Plaintiffs and Class

Members and continued acceptance of Private Information and storage of other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

122. Defendant acted in bad faith and/or with malicious motive in denying Plaintiffs and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them substantial injury in an amount to be determined at trial.

COUNT V
INVASION OF CONFIDENCE
(On Behalf of Plaintiffs and All Class Members)

123. Plaintiffs incorporate by reference and re-allege each and every allegation set forth above in paragraphs 1 through 14 and paragraphs 23 through 59 as though fully set forth herein.

124. At all times during Plaintiffs' and the Class's interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and the Class's Private Information that Plaintiffs and the Class entrusted to Defendant.

125. As alleged herein and above, Defendant's relationship with Plaintiffs and the Class was governed by terms and expectations that Plaintiffs' and the Class's Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

126. Plaintiffs and the Class entrusted Defendant with their Private Information with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized third parties.

127. Plaintiffs and the Class also entrusted Defendant with their Private Information the explicit and implicit understandings that Defendant would take precautions to protect that Private Information from unauthorized disclosure.

128. Defendant voluntarily received in confidence Plaintiffs' and the Class's Private Information with the understanding that Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

129. As a result of Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiffs' and the Class's Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and the Class's confidence, and without their express permission.

130. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiffs and the Class have suffered damages.

131. But for Defendant's disclosure of Plaintiffs' and the Class's Private Information in violation of the parties' understanding of confidence, their Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiffs' and the Class's Private Information as well as the resulting damages.

132. The injury and harm Plaintiffs and the Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and the Class's Private Information. Defendant knew or should have known its methods of accepting and securing Plaintiffs' and the Class's Private Information was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiffs' and the Class's Private Information.

133. As a direct and proximate result of Defendant's breach of its confidence with Plaintiffs and the Class, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud,

and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of current and former patients; and(viii) present and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

134. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and the Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT VI
Missouri Merchandise Practices Act
Mo. Rev. Stat. §§ 407.010, *et seq.*
(On behalf of Plaintiffs and Missouri Subclass Members)

135. Plaintiffs repeat and re-allege the factual allegations set forth in paragraphs 1 through 14 and paragraphs 23 through 59 and incorporate the same as if set forth herein.

136. Defendant is a "person" as defined by Mo. Rev. Stat. § 407.010(5).

137. Defendant engaged in "sales" of and "advertisements" for "merchandise" in Missouri and engaged in trade or commerce directly or indirectly affecting the people of Missouri, as defined by Mo. Rev. Stat. § 407.010(1), (4), (6) and (7).

138. Defendant engaged in unlawful, unfair, and deceptive acts and practices, in connection with the sale or advertisement of merchandise in trade or commerce, in violation of Mo. Rev. Stat. § 407.020(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;
b. Failing to identify and remediate foreseeable security and privacy risks and properly improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
d. Misrepresenting that it would protect the privacy and confidentiality of Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;
e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Subclass Members' Private information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
f. Omitting, suppressing, and concealing the material fact that it did not properly secure Subclass Members' Private Information; and
g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

139. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

140. Defendant intended to mislead Missouri Subclass Members and induce them to rely on its misrepresentations and omissions.

141. Defendant acted intentionally, knowingly, and maliciously to violate Missouri's Merchandise Practices Act, and recklessly disregarded Missouri Subclass Members' rights. Defendant's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

142. As a direct and proximate result of Defendant's unlawful, unfair, and deceptive acts and practices, Missouri Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private information; overpayment for Defendant's services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

143. Plaintiffs, on behalf of Missouri Subclass Members, seek all monetary and non-monetary relief allowed by law, including actual damages, punitive damages, attorneys' fees and costs, injunctive relief, and any other appropriate relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seek judgment against Defendant, as follows:

(a) For an order determining that this action is properly brought as a class action and certifying Plaintiffs as the representatives of the Class and their counsel as Class Counsel;

(b) For an order declaring the Defendant's conduct violates the laws referenced herein;

(c) For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;

(d) For damages in amounts to be determined by the Court and/or jury;

(e) An award of statutory damages or penalties to the extent available;

(f) For pre-judgment interest on all amounts awarded;

(g) For an order of restitution and all other forms of monetary relief; and

(h) Such other and further relief as the Court deems necessary and appropriate.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims in this Class Action Complaint so triable.

Dated: May 23, 2024

Respectfully submitted,

CAREY, DANIS & LOWE

By: */s/ James J. Rosemergy*
James J. Rosemergy
8235 Forsyth, Suite 1100
St. Louis, MO 63105
Telephone: (314) 725-7700
Facsimile: (314) 721-0905
Email: jrosemergy@careydanis.com

Mark S. Reich*
Courtney E. Maccarone*
Gary I. Ishimoto*
LEVI & KORSINSKY, LLP
33 Whitehall Street, 17th Floor
New York, NY 10004
Telephone: (212) 363-7500
Facsimile: (212) 363-7171
Email: mreich@zlk.com
Email: cmaccarone@zlk.com
Email: gishimoto@zlk.com

**pro hac vice* forthcoming

Counsel for Plaintiffs